

シャドウコピーを利用した ファイル管理システムの提案と評価

松高 直輝^{1,a)} 松本 隆¹ 上原 哲太郎² 佐々木 良一¹

受付日 2017年11月25日, 採録日 2018年6月8日

概要: 近年, 半導体を用いた記憶装置である SSD (Solid State Drive) の普及が進んでいる. SSD は Trim により削除ファイルを完全消去することでデータ処理の高速化を実現している. その反面, 1 度ファイルを削除してしまうと復元できなくなるという問題をかかえている. そのため, 定期的なデータのバックアップをとることが, PC のユーザにとっても, デジタル・フォレンジックの専門家が不正の証拠を確保するためにも不可欠になる. 本研究では, ボリュームシャドウコピーサービスを利用したバックアップを推奨する. しかし, 従来までのシャドウコピー関連ツールは, 操作方法が分かりにくいとともに, ランサムウェア等の脅威に対応するための機能が実装されていなかった. そこで本稿は, 基本的なバックアップ機能に加え, 不正なシャドウコピーの削除に対応する機能を備えたファイル管理システム「VSSManager」を提案する. 提案するシステムは, (1) 個人向けバックアップ機能と, (2) 組織向けシャドウコピー管理機能から構成される. 本システムがユーザにとって簡単に操作できること, シャドウコピー保護のための要件を満たすことができるかを確認するために, (1) 個人向けバックアップ機能のプロトタイプを開発し, 実験と評価を行ったのでその結果も報告する.

キーワード: シャドウコピー, バックアップ, SSD, デジタル・フォレンジック, ランサムウェア

Proposal and Evaluation of Files Management System Using Shadow Copy

NAOKI MATSUTAKA^{1,a)} TAKASHI MATSUMOTO¹ TETSUTARO UEHARA² RYOICHI SASAKI¹

Received: November 25, 2017, Accepted: June 8, 2018

Abstract: In recent years, Solid State Drive (SSD) have started to replace Hard Disk Drive. An SSD is a high-speed storage device with a Trim. However, an SSD cannot recover deleted files. Therefore, the user is required to backup data for protection. It is also essential for digital forensics experts to secure evidence of fraud. In this research, we recommend backup using the Volume Shadow Copy Service (VSS). However, although it has tools for backup, they are complicated to use. In addition, they do not have functions for dealing with ransomware and internal crime in an organization. Therefore, we propose file management system named VSSManager, which has functions for basic backup and unauthorized deleting shadow copy. VSSManager consists of (1) a backup function for personal use and (2) shadow copy management function for the organization. Then, we develop prototype of (1) a backup function for personal use and evaluate it from viewpoint of usability and functions requirements.

Keywords: shadow copy, backup, SSD, digital forensics, ransomware

1. はじめに

近年, HDD に代わる記憶装置として Solid State Drive (以後, SSD) の普及が進んでいる. SSD は半導体を用いた記憶装置であり, HDD のようにディスク上でヘッドを

¹ 東京電機大学
Tokyo Denki University, Adachi, Tokyo 120-8551, Japan

² 立命館大学
Ritsumeikan University, Kusatsu, Shiga 525-8577, Japan

a) 16fmi31@ms.dendai.ac.jp

移動させる時間がないため、ファイルを高速に読み込むことができる。SSD に記録できる容量の増加や性能の向上が進み、SSD の普及率は今後も高まると思われる。その一方、SSD にはデジタル・フォレンジックやファイル誤削除に対しての課題がある。なお、本稿におけるデジタル・フォレンジックとは「種々のインシデントが発生した際に、将来行われうる裁判で証拠として使用できるようにするための電磁的記録の収集や分析の技術およびその手順」[1] とする。

SSD には Trim と呼ばれる機能がある。Trim は、不要になったファイルが書き込まれているセクタを検知し、自動的に空きブロックの作成を行う。これにより SSD は、半導体の欠点である書き込み速度の低下を抑えている。その反面、Trim によって削除したファイルが復元できなくなるという問題をかかえている。HDD や USB メモリ等の Trim が存在しない記憶装置の場合、ファイルを削除してもその時点では実データは消去されないため復元が可能である。しかし、Trim を有効にした記憶装置の場合、ファイルが削除されると OS が自動的にそれを不要なファイルと認識し、実データを完全消去してしまう。インシデントの証拠となる電子的記録が Trim によって失われるため、SSD のデジタル・フォレンジックが困難になる。同様に、ユーザが誤ってファイルを削除してしまった場合も復元することは困難である。山前らは SSD における消去ファイルの可能性について実験した [2]。その結論では、Trim 有効時は削除直後であってもいっさい復元できず、Trim 無効時であってもファイルは約 24 時間しか残らないということを述べている。

SSD ではファイル復元が不可能であるため、SSD のデジタル・フォレンジックでは、証拠となるデータをつねに保護する必要がある。また、誤削除に関してもヒューマンエラーである以上は、簡単にファイルを復元できる仕組みが必要である。本研究は、これらの課題をバックアップシステムによって解決を図る。バックアップ方式としては、2.2 節に示すように様々な方式があるが、ここでは、バックアップに必要な容量が少なく済むボリュームシャドウコピーサービスの利用を前提とする。しかし、シャドウコピーを利用したバックアップツールには以下のような問題があった。

- (a) 既存のツールは、設定や復元のための操作が分かりにくく、実装されている機能が不十分である。そのため PC の持ち主がバックアップの設定や復元を行うことが困難であった。
- (b) 近年のランサムウェアはファイルを暗号化した後、シャドウコピーの消去を試みていることが確認されている。シャドウコピーを消去されるとファイルは復元できなくなる。
- (c) 組織での利用を考慮した場合、不正者が意図的にシャ

ドウコピーを消去することで証拠隠滅を図ることが考えられる。不正の証拠を消去されるとデジタル・フォレンジックを適用できない可能性がある。

本研究は、SSD におけるデジタル・フォレンジック等の問題とランサムウェアによる問題を取り上げ、シャドウコピーを用いた新たなバックアップシステムによって解決させるものである。本稿が説明する各機能は、従来までに見られる基本的な手法を用いているが、それらを組み合わせることでより有用性のあるシステム “VSSManager” を提案する。VSSManager は上記した問題を解決するために次のような機能を持つように開発する。

- (i) エンドユーザが容易にバックアップを行うことができ、シャドウコピーからファイルを復元できる機能
- (ii) ランサムウェアからシャドウコピーを保護する機能
- (iii) 組織内部の不正者が容易にシャドウコピーを消去できない仕組み、また、シャドウコピーを消去しようとしたときに管理者がその情報を知ることができる機能

なお、(ii) が対応するのは近年増加している「暗号化型ランサムウェア」とする。これらを実現するための方式を確立するとともに (i) と (ii) のプロトタイプを開発し、有効性の評価を行った。その結果、有効性の見通しが得られたので報告する。

2. 関連技術

2.1 バックアップ方式

一般的なバックアップの方法として外付け HDD を用いて複製したファイルを保存することがあげられる。この場合、ユーザはバックアップ用の媒体を別途用意する必要がある、コストがかかる。そこで外部媒体を利用せず、オンラインでバックアップを行うことも増えている。吉田らは Peer to Peer ネットワークを利用したバックアップシステムを提案している [3]。ネットワーク上の複数の端末を利用し、冗長性、分散性、セキュリティを達成したデータ管理を実現している。また、Rahumed らはクラウド上で安全かつ効率的なバックアップシステムの提案をしている [4]。ファイルごとのバージョン管理や暗号化により、ユーザのファイルを安全に保護することを目的としている。ただ、オンラインを利用したバックアップ方法は、ファイルをアップロードすることに時間がかかるため、多数のファイルや容量の大きなファイルをバックアップすることには向いていない。そこで本研究では、バックアップの処理時間が短く、かつ比較的データ容量を抑えることができるボリュームシャドウコピーサービスの利用を推奨する。

2.1.1 ボリュームシャドウコピーサービス

ボリュームシャドウコピー (以後、VSS) は、Windows OS のバックアップ機能である。VSS はドライブ上で更新されたファイルの変更点をシャドウコピー (以後、SC) というシステムファイルに書き込み、それを専用の領域に保存す

る [5]. これにより, ファイルを削除・上書きした場合でも VSS を利用することで元のファイルに戻すことができる. SC の作成には, ドライブの状態を記録するスナップショットが必要である. スナップショットを記録後, ファイルが削除・変更されるたびに記録されているスナップショットと現在のドライブとの差分を SC に保管する. この処理はバックグラウンドで行われるため, ユーザが処理時間を気にすることなくバックアップが行える. また, 変更された部分のみを保管するため, バックアップに要するデータ容量を抑えることができる. 加えて, 通常のバックアップでは実行中のファイルやロックされているファイルのバックアップをとることができないが, VSS はファイルの状態にかかわらずバックアップをとることができる. Pecherle らは VSS を利用し, アプリケーションが保管しているデータを初期状態に戻す手法を提案している. Web ブラウザの Cookie やチャットアプリのメッセージアーカイブ等を PC 上に残さないことで, ユーザに関する機密情報を保護することができるとしている [6]. SC は削除されたファイルを復元し, コンピュータ上でどのような処理が行われていたか解析することができるため, デジタル・フォレンジックにとっても重要なデータである [7]. 1 章で述べた SSD におけるデジタル・フォレンジックの課題に対応するためにも, SC を保護する仕組みが必要であると考えられる.

2.2 ランサムウェア対策

ランサムウェアは, 感染したコンピュータへのアクセスを制限し, 制御を解除するためにユーザに身代金を支払うように要求する不正プログラムである. ランサムウェアは, コンピュータの画面をロックする「画面ロック型」とファイルを暗号化する「暗号化型」の 2 つの攻撃タイプがある. 近年は, 暗号化型ランサムウェアによる攻撃が急増している [8]. ランサムウェアによってファイルが暗号化されてしまうと, それを復元することは困難になる. この問題に対し, 竹林らはライブフォレンジックを用いた復号方法を開発した [9]. ランサムウェアは様々な暗号アルゴリズムを用いるが, これらを復元できる可能性があることを示している. また, ランサムウェアを検知する方法として Mbol らは, 多数のファイルにアクセスし, それらを暗号化しようとするプロセスを検出する手法を提案している [10].

現在, 様々な手法でランサムウェアの被害を減らす研究が多数行われている. しかし, 同時にランサムウェアも進化し続けており, 絶対的な対策というのは存在しない. そのためコンピュータを利用するユーザは, ソフトウェアを最新の状態に保つ等, マルウェアに感染させないことが求められる. また, ファイルのバックアップを定期的に行っておくことで, 暗号化された際の被害を最小限に抑えることも大切である. SC によるバックアップも有効であるが, 暗号化後に SC の削除を試みるランサムウェアも存在して

おり, 従来の SC 関連ツールではこれらの攻撃に対応することができない.

3. SC を利用したファイル管理システムの提案

3.1 システムの構成

1 章で述べた理由により, 本稿が提案するシステム (以後, VSSManager) は, 次のような操作性・機能が必要であると考えた.

- ① エンドユーザが容易に SC の作成やファイルの復元を行える.
- ② ランサムウェア等の悪意ある攻撃から保管している SC を保護する.
- ③ 組織内の人間が自身にとって都合が悪い SC を勝手に削除できないようにするため, 削除を行うと組織のデータ管理者にその情報が通達される.

① と ② は, 「エンドユーザ用バックアップ機能」として開発する. ① は一般ユーザが容易に SC の作成・設定, 復元を行えることを目標とし, 既存のバックアップツールの操作性の改良案を検討することで達成させる. ② はランサムウェアや悪意ある人間が SC 削除を行えないように動作の検知と停止を行う.

VSSManager を企業等の組織内で利用する場合は, 「エンドユーザ用バックアップ機能」に加え, ③ の「SC 管理機能」を追加する. 一般ユーザは「エンドユーザ用バックアップ機能」を利用し, 管理者が「SC 管理機能」を用いて社内 PC を一元的に管理することができる. また, 一般ユーザが SC の削除を行う際, 管理者へ許可を求める操作を行うことで不正な削除をさせない仕組みをとる.

本研究は, ユーザに定期的なバックアップを促し, インシデント時の操作を容易に行えることを目的とした ① の機能により, バックアップシステムの有用性を示す. また, 従来にはなかった ②, ③ の機能を有することで, 外部・内部からの攻撃を防ぐバックアップシステムの新規性を示す.

以下, 図 1 に提案する VSSManager の構成を示す. 次節以降は各機能の詳細について述べる.

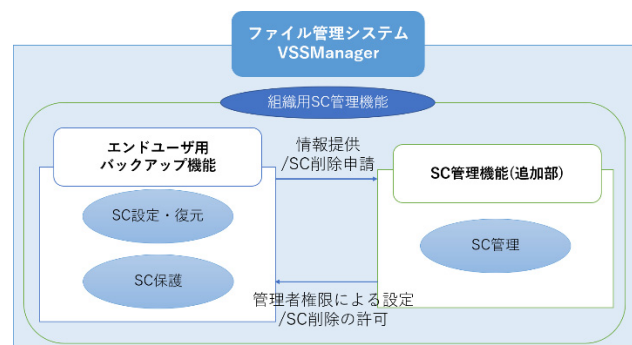


図 1 SC を利用したファイル管理システムの構成

Fig. 1 The configuration of files management system using shadow copy.

3.2 エンドユーザ用バックアップ機能

我々は、エンドユーザ向けのバックアップ機能として、一般ユーザが容易に操作でき、かつ、近年のランサムウェアに対応する力を高めるために、次のような操作性・機能を実現させた。

(a) 定期的なバックアップを手助けするために、容易に SC の設定や復元が行えるユーザビリティ

(b) ランサムウェアの攻撃から SC を保護する機能

(c) ランサムウェアに感染後、感染前の SC を自動的に探し出すことで、ユーザの作業量を減らす仕組み

(a) はバックアップに関する基本的な機能であり、従来のバックアップツールと同様である。ただ、ユーザがバックアップの初期設定（バックアップを行う頻度や SC 保管領域の設定等）を適切に行えることや、誤削除やランサムウェアによるファイル暗号化からファイルを復元する操作が容易に行えるためには、適切なユーザインタフェースを実現する必要があると考えた。そこで、バックアップ機能の操作性を確保するために、既存ツールの操作面を吟味し、実装するユーザインタフェースの考案を行う。3.2.1 項では、SC を利用してバックアップを行う既存ツールとして「以前のバージョン」、「ShadowExplorer」の概要と操作性・機能面の課題について述べる。そして 3.2.2 項では、その課題点を考慮した VSSManager の機能とインタフェースを考案する。

(b) と (c) は、従来のツールにはなかったランサムウェアに対応する力を持たせるための機能である。これらの機能を備えることで、ランサムウェアに感染した場合であっても、復元作業にかかる負担を減らすことができると考えた。SC 保護機能の概要は 3.2.3 項で述べる。

3.2.1 既存の SC 関連ツール

図 2 に示す画面は、Windows OS (Vista, 7, 10) に備わっている「以前のバージョン」と呼ばれる機能である。「以前のバージョン」は、SC 作成、SC 保管領域の設定、ファイル復元を行うことができる [11]。図 3 に示す ShadowExplorer は、SC からバックアップファイルを一覧

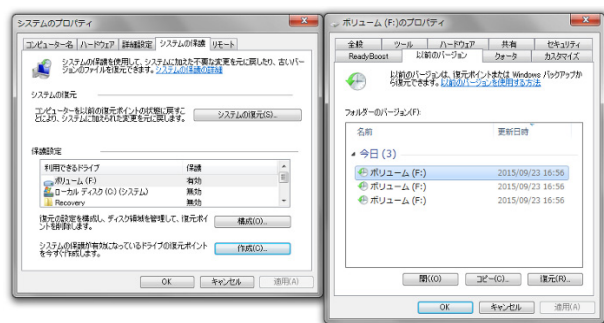


図 2 「以前のバージョン」の画面。システムのプロパティ（左）とボリュームのプロパティ（右）

Fig. 2 The screens of Previous Versions. System Properties and Volume Properties.

で表示し、その中から任意のファイルを復元できるツールである [12]。

「以前のバージョン」では SC の設定や復元を行うことができるが、すべての機能を使用するためには複数の画面から操作する必要がある。具体的には、SC 作成と設定を行うには「システムの保護」、ファイル復元を行うには「ボリュームのプロパティ」の画面を操作する。SC に関する機能がまとめられていないため、ユーザが操作に戸惑うことが懸念される。また、SC 作成機能は、複数のドライブが存在する場合、すべてのドライブで SC が作成されてしまい、ユーザの意図に反してドライブ容量を圧迫してしまう可能性がある。SC 削除機能に関しても複数 SC が存在する場合でも選択して削除することができず、ドライブ全体の削除が実行されてしまう。ShadowExplorer はファイル復元を目的としたツールであり、SC 作成や設定を行うことができない。また、どちらのツールもフォルダを復元する際、フォルダ内のファイルが実行されていると復元することができず、処理が中断されてしまうことがあった。加えて、既存ツールは SC 削除攻撃に対応する機能を有しておらず、ランサムウェア等の攻撃を受けた場合にはファイルの復元を行うことができない。表 1 に既存ツールが実装している機能を示す。表 1 より、既存ツールは機能が分散しており、一元的に機能を扱えないため非効率な印象を受ける。

3.2.2 SC 設定・復元機能の検討

VSSManager が実装するバックアップの基本機能は、「SC

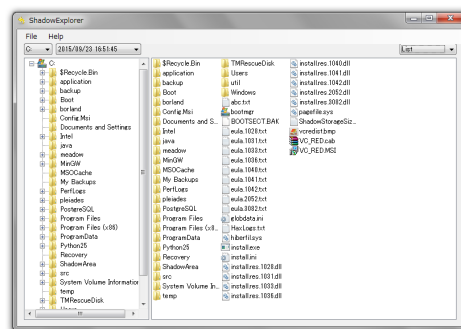


図 3 ShadowExplorer の画面

Fig. 3 The screen example of ShadowExplorer.

表 1 既存ツールの機能

Table 1 The functions of existing tools.

機能	以前のバージョン		Shadow Explorer
	システム	ボリューム	
SC作成	△	-	-
SC削除	△	-	-
保管設定	○	-	-
ファイル検索	-	○	
ファイル復元	-	○	○

※○：実装，△：機能として不十分，-：実装なし

表 2 既存ツールの課題と改善内容

Table 2 The problems of existing tools and the improvement methods.

既存ツールの課題点	改良方法
SC 作成やファイル復元の機能を一括で使うことができない	基本機能を一元的に実装することで操作の効率化を図った
複数のドライブが存在する場合、すべてのドライブで SC 作成が実行されてしまう	複数のドライブが存在する場合は、SC 作成時にドライブを選択できるようにした
SC を選択して削除することができず、ドライブ全体での削除しかできない	複数の SC が存在する場合は、ユーザが SC を選択して削除できるようにした
フォルダ等を復元する際、フォルダ内のファイルが実行されていると復元することができない	実行中のファイルが存在する場合は、ユーザにそのファイルの情報を提示し、実行の停止を行えるようにした
SC 削除攻撃に対応していないため、ランサムウェア等の被害に対応することができない	3.2.3 項で説明する SC 保護機能を実装することで SC 削除攻撃に対応できるようにした

の作成・削除」「SCの保管設定」「ファイルの復元」である。「SCの保管設定」は保管領域の拡大・縮小等の操作を行う。これらの基本機能を一元的に実装することで、効率的にバックアップや復元を行うことができる。加えて、定期的なバックアップを手助けするためにSC作成のスケジュールを設定できる機能を新たに実装する。また、3.2.3 項で機能の詳細を後述するが、ランサムウェア感染後にドライブを復元する際、感染前のSCを自動的に探す機能を持たせた。これは、ユーザが適切なSCを探す際の負担を減らすことができると考えたためである。そして、既存ツールの課題点をふまえたうえで、新たなユーザインタフェースを実装する。表2に既存ツールの課題点とそれに対する改善方法を示す。

3.2.3 SC 保護機能の概要

近年のランサムウェアは SC の削除を試みており、ユーザに SC による復元をさせないようにしている。SC はシステムファイルであり、アクセス権限がないユーザは削除することができない。そのため、SC を削除するには、表 3 に示す VSS へのアクセス権限が付与されているファイルを使用する必要がある、それ以外の削除方法は存在しないと考える。実際、ランサムウェアはこれらのファイルを利用して SC 削除を試みている。一例をあげると、ランサムウェア WannaCrypt は `vssadmin.exe` と `wmic.exe` を用い

表 3 SC 削除に使用されるファイル

Table 3 The files used for deleting shadow copy.

ファイル名	詳細
vssadmin.exe	VSS に関する処理 (SC 作成や SC 削除) をコマンドで実行するためのツール
wmic.exe	WMI と呼ばれる Windows のシステム管理を行うコマンドラインツール
vssapi.dll	VSS に関連する API 群をまとめた DLL ファイル
SystemPropertiesProtection.exe	Windows OS の標準搭載機能「システムの保護」

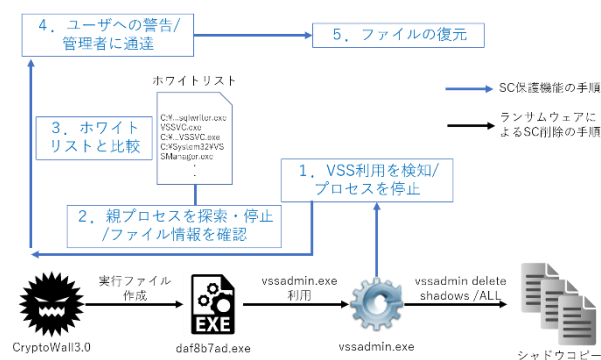


図 4 SC 保護の手順

Fig. 4 The procedure for protecting shadow copy.

て SC 削除コマンドを実行する [13]. また, ランサムウェア Locky の亜種である Zepto は vssapi.dll を用いて API を呼び出して SC 削除を試み, これに失敗すると vssadmin.exe による SC 削除を行う [14]. そのため, SC を作成しているだけでは, 対策として不十分であるといえる. また, 組織での利用を考える場合, 不正者が VSSManager を介さずに SC 削除を行う可能性がある. VSSManager はこれらの攻撃手法に対応するため, 以下の手順 1~4 による保護機能を実装した. 図 4 には SC 保護機能の手順に関する図解を示す. なお, 正規のファイルによる VSS の利用を妨げてしまわないように, 事前にホワイトリストを設定しておき, 検知の対象から外すことにする. ホワイトリストには, 正規に VSS を利用するファイルのパス情報を登録する. ファイルパスによる判断を行うことで, 攻撃者が正規ファイルと同名のファイルを作成した場合であっても, ファイルパスが異なれば検知することができる. 表 4 に Windows7, 10 において正規に VSS を利用するファイルを示す. また, ホワイトリストには VSSManager に関連するファイルも

表 4 正規に VSS を利用するファイル (Windows7, 10)
Table 4 The files using VSS without injustice (Windows7, 10).

ファイル名	詳細
svchost.exe	WindowsOS のサービスを受け持つシステム機能
SearchIndexer.exe	ファイル検索を高速化するための機能
TrustedInstaller.exe	WindowsOS の更新プログラム等をインストールする機能
sqlwriter.exe	SQLServer のバックアップと復元に関する機能
VSSVC.exe	VSS を利用するための実行ファイル

登録することとする。

(手順 1) コンピュータで起動しているプログラムを監視する。表 3 に示したファイルの使用を検知した場合は、使用元のファイルが生成したプロセスを停止させる。

(手順 2) 停止させたプロセスを参照し、親プロセスが存在するか確認する。親プロセスが存在する場合は、プロセスを遡って SC 削除を図ろうとした大元のファイルを調査する。

(手順 3) 手順 2 で収集した親プロセスのファイルパス情報をホワイトリストと比較する。ホワイトリストとの照合がとれた場合は、プロセスの処理を再開させる。照合がとれなかった場合は手順 4 に進む。

(手順 4) ユーザに対し、VSSManager を介さずに SC の削除が行われようとしていることを警告する。また、組織での利用の場合、手順 2 で得た情報を管理者に通知する。

(手順 5) ランサムウェアによって暗号化されたファイルを復元する際には、手順 2 で特定したファイルが存在しない SC (ランサムウェアに感染する前に作成した SC) を提示する。

3.3 SC 管理機能

組織での利用を考えた場合、不正者が意図的に SC を消去することで証拠隠滅を図ることが考えられる。不正の証拠が消去されるとデジタル・フォレンジックを適用できない可能性がある。そこで VSSManager では、不正者が容易に SC を消去できない仕組みを構築し、SC を消去しようとしたときに管理者がその情報を知ることができる機能を実装する。

図 5 に不正な SC 削除、正規のユーザから SC 削除の申請があった場合の処理の流れを示す。(1) VSSManager を介さない SC 削除が行われた場合、SC 保護機能によってプロセスの停止とその情報を管理者に提供する。(2) 正規の理由で SC を削除したい場合には、管理者に SC 削除を申請する。(3) 管理者はエンドユーザから削除に関する理由を受け取り、削除処理を許可するか拒否するかを判断する。

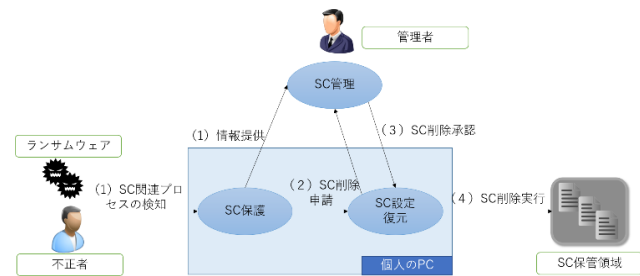


図 5 組織内部での SC 削除処理の流れ
Fig. 5 The procedure for deleting shadow copy on the organization.

表 5 既存ツールと VSSManager の比較
Table 5 The comparison of existing tools and VSSManager.

機能	以前のバージョン		Shadow Explorer	VSS Manager
	システム	ポリシー		
SC 作成	△	-	-	○
SC 削除	△	-	-	○
保管設定	○	-	-	○
ファイル復元	-	○	○	○
SC 保護	-	-	-	○
SC 管理	-	-	-	○

※○：実装，△：機能として不十分，-：実装なし

(4) 管理者からの許可が下りた場合は SC 削除を実行する。

本稿が提案する SC 管理機能は、従来までの SC 削除方法よりも大幅に手順が増加する。しかし、組織での利用を想定した場合、エンドユーザが SC を削除しなければならない場面はほとんどないと考えられる。正規の理由として「容量の圧迫」等が考えられるが、これは管理者側から SC 保管領域を事前に指定させる仕組みにするため適切な理由にならない。その他、重大な理由によって SC 削除を行わなければならない場合のみ手間をかけさせても申請を行わせる。ユーザが容易に削除を行えない仕組みにすることで、結果的に SC を保護することにつながると思う。

4. プロトタイプモデルの開発と評価

4.1 プロトタイプの開発

本研究が提案する機能について評価を行うために VSSManager のプロトタイプを開発した。表 5 に既存ツールと VSSManager が有する機能について示す。VSSManager は基本的なバックアップ機能を一元的に実装し、従来までにはなかった SC 保護機能と SC 管理機能を有していることを示している。図 6 は VSSManager のメイン画面であり、ファイルの復元を行う。図 7 は VSSManager の設定画面とランサムウェア検索画面である。設定画面では、SC 保管領域の設定や SC 作成・削除、SC 保護機能 (ホ

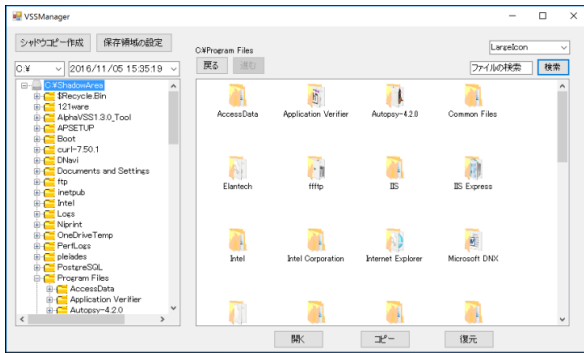


図 6 VSSManager のメイン画面
Fig. 6 The main screen of VSSManager.

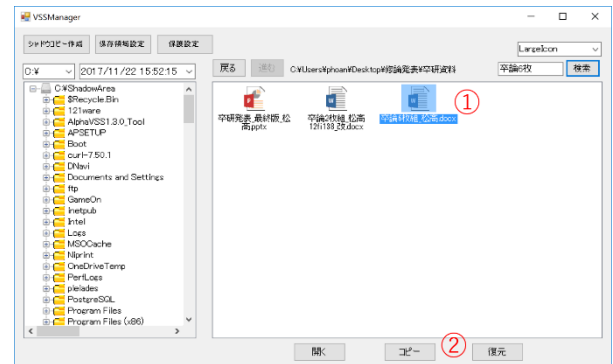


図 9 VSSManager の復元画面
Fig. 9 The restored screen using VSSManager.

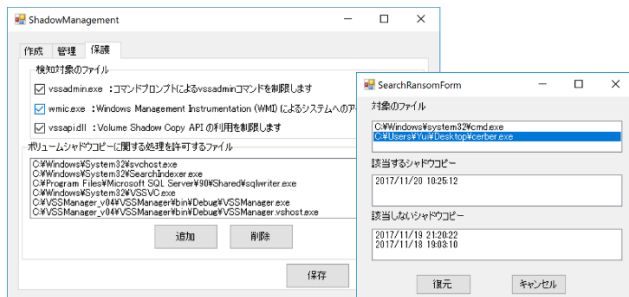


図 7 設定画面・ランサムウェア検索画面
Fig. 7 The screens for setting and searching ransomware.

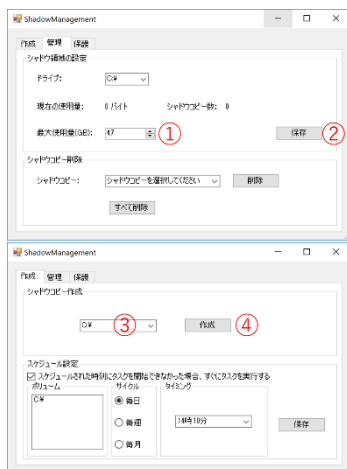


図 8 SC 保管領域設定 (上), SC 作成の頻度設定 (下)
Fig. 8 The screens of setting storage area and creating shadow copy.

ワイトリスト等)の設定を行う。ランサムウェア検索画面では、ランサムウェアから SC を保護した後、ドライブを復元する際に利用する。現在、VSSManager は Windows7, 10 での動作を確認している。

4.2 プロトタイプの評価

実装した各機能が要件を満たしているかを確認するために評価アンケートと実験を行った。本稿では、「エンドユーザ用バックアップ機能」のユーザインタフェースに関する評価とランサムウェアからの防御実験の結果について述べる。

4.2.1 バックアップ操作の評価

図 8 に VSSManager の SC 作成と設定画面を示す。SC の保管領域の設定をする際は、① 使用領域を容量 (GB) で設定し、② 変更を確定する。SC を作成する際は、③ 対象のドライブを選択して ④ 作成ボタンを押下するだけで作成できる。「以前のバージョン」では「システムの保護を有効にする」設定や SC 作成時に SC の説明を入力する必要があったが、VSSManager ではこれらの操作を省くことでステップ数を減らした。

図 9 に VSSManager のファイル復元画面を示す。VSSManager では SC を選択した後、① 復元したいファイルを左のフォルダツリーから探し出し、② そのファイルをコピーするか、元の場所に上書きするかを選択することができる。VSSManager はファイル名による検索機能を実装しており、また、フォルダ間の遷移がしやすいようにファイルパスの表示や遷移操作の取り消し機能等のユーザインタフェースを実装している。

VSSManager のエンドユーザ用バックアップ機能が一般ユーザにとって使いやすいツールであるかを確認するため、テストユーザに VSSManager を使ってもらいアンケートを集計した。また、従来までの SC 関連ツールと比較して操作性が改善されているかを評価するために「以前のバージョン」、ShadowExplorer も同時に使用してもらった。アンケートでは、バックアップの基本機能である「SC 作成」「保管設定」「ファイル復元」を操作してもらい、各機能の使いやすさを 5 段階の点数で付けてもらう。また、使用時に感じたことを意見してもらう。ここでの「ファイル復元」は、「復元したいファイルを探すところから復元するまでの一連の操作」を指している。

評価にあたり、テストユーザとして学生 10 人に協力を仰いだ。表 6 に評価結果を示す。なお、「非常に使いにくい」を「1」、「非常に使いやすい」を「5」として、その 5 段階評価の平均値を載せている。なお、ShadowExplorer は「SC 作成」と「保管設定」に対する機能が備わっていないため評価対象から外している。

表 6 テストユーザによる UI 評価

Table 6 The evaluation of interface obtained by test users.

機能	以前のバージョン	Shadow Explorer	VSS Manager
SC 作成	2.6	-	4.7
保管設定	1.5	-	4.9
ファイル復元	3.4	3.0	3.6

表 7 ランサムウェアと SC 保護機能の実験結果

Table 7 The result of experiment on protection function against ransomware.

ランサムウェア	SC 削除に使用されるファイル	検知結果
Locky	vssadmin	○
Cryptowall	vssadmin	○
CryptoLocker	vssadmin	○
TeslaCrypt	wmic	○
Cerber	vssadmin, wmic	○
WannaCrypt	vssadmin, wmic	○
Zepto	(vssapi) vssadmin	○

表 6 より VSSManager は既存ツールよりも操作しやすくなっていることが分かる。これは 3.2.2 項で検討したユーザインタフェースによって直感的な操作性を実現できたためであると考えられる。ユーザからの意見では、「SC の作成までの手間がかからない」「既存ツールに比べて操作が分かりやすい」という評価が得られた。ただ、「ファイル復元」はあまり評価が変わらなかった。ユーザはふだん Windows エクスプローラの画面でファイル操作を行っているため、「以前のバージョン」の方が比較的容易に扱えたのではないかと考えられる。そのため、VSSManager の改良としてファイル復元の際の画面を Windows エクスプローラのレイアウトに近づける等の案があげられる。

4.2.2 SC 保護機能の評価

VSSManager がランサムウェアによる削除攻撃から SC を保護することができるかを確認するために実験を行った。実験環境、手順は以下のとおりである。

1. 仮想環境上のコンピュータ (Windows 7) で VSSManager を起動し、SC 保護機能を有効にする。
2. SC 削除攻撃を行うランサムウェアをコンピュータに感染させる。
3. VSSManager がランサムウェアによる SC 削除を検知し、プロセスの停止を行えるか、また警告画面を適切に表示できるかを確認する。

実験に用いたランサムウェアは、SC 削除攻撃を行うと確認されている Locky, Cryptowall, CryptoLocker, TeslaCrypt, Cerber, WannaCrypt, Zepto である。表 7 に実験結果を示す。その結果、VSSManager はすべてのランサム

ウェアにおいて SC 削除を漏れなく検知し、そのプロセスを停止させることに成功した。このうち、Zepto は vssapi.dll と vssadmin.exe を利用した SC 削除を行うと認識していたが、今回の実験では vssadmin.exe での削除しか行われず、vssapi.dll は使用されなかった。しかし、vssapi.dll を検知してプロセスを止める機能は問題なく動くことを確認しており、実際に vssapi.dll を利用した際には、そのファイルを検知することができている。これらの結果から、ランサムウェアによる不正な SC 削除に対して提案手法が有効であるといえる。また、組織内部の不正者がランサムウェアと同手法の攻撃を行った場合でも対応できると考える。

5. 今後の展望

SC 保護の実験ではファイルの暗号化と SC 削除を行うとされる exe ファイルのみを利用して検証したが、今後は実際の感染を想定した環境での実験を行いたい。それにより、SC 削除検知時に親プロセスを最大限まで特定することができ、ランサムウェアが存在しない SC を正確に特定できると考える。

現状のランサムウェアであれば、3.2.3 項で示した SC 保護機能の仕組みで十分に対応できると考えている。しかし、将来的には、ホワイトリストのファイル（正規ファイル）を騙るマルウェア等への対応を考えたい。現時点で考えられるリスクとその対応策は次のとおりである。

a) 正規ファイルがマルウェアに上書きされるリスク

攻撃者がホワイトリストに登録されているファイルパス情報を取得し、正規ファイルと同名のファイルをディレクトリ上に作成する可能性がある。そのため、将来的には正規ファイルを監視対象とし、ファイルの変更・削除を検知する仕組みを実装する。

b) マルウェアが正規ファイルに悪意ある命令を行い、SC 削除を実行するリスク

攻撃者が正規ファイルを乗っ取り、悪意ある命令を実行させるリスクが考えられる。これに関しては、外部からの命令を実行させないためにも OS やソフトウェアの脆弱性を放置せずにアップデートするという基本的な対応が必要である。本システムにおける対策としては、検知した親子プロセスの関係性を見ることで、命令の正規性を判断することが考えられる。具体的には、正規ファイルが VSS を利用した際の親子プロセス関係をホワイトリスト化する。一例をあげると、本システムが VSS を利用する際には「VSSManager.exe → vssapi.dll」というプロセス関係が検知される。ここで、マルウェア (Ransomware.exe) が本システムに SC 削除命令を出した場合、「Ransomware.exe → VSSManager.exe → vssapi.dll」というプロセス関係が検知される。このプロセス関係を見ると、VSSManager の親プロセスに許可されていないファイルが存在していない

ことが分かる。これにより、正規ファイルを経由したマルウェアによる攻撃を判断できると考える。

上記の対応策を実装した場合、各処理に影響がでないか確認するために処理速度を計測した。(a)の対応策を実施した場合は、VSSManagerの起動時に監視するファイルを登録するために約1,200ミリ秒かった。また、(b)の対応策を実施した場合は、SC保護機能のホワイトリスト参照時に約3ミリ秒かった。この結果から、機能を拡張した場合でもVSSManagerの処理には大きな影響はないと考える。ただし、OSやソフトウェアのアップデート時に誤検知の恐れや監視対象のファイルの数によって処理時間が増加する等の欠点がある。そのため、これらの機能は欠点を考慮したうえで拡張をする必要があると考える。

SC管理機能は機能構成の提案を行ったが、今後、組織内のシステムの中でVSSManagerを安全に利用するためには、ユーザ端末と管理者端末間の通信の安全性を確立する等、他のサブシステムと同様にシステム全体としてみた場合のリスク分析を実施することが望ましい。

6. おわりに

SSDのファイル復元、デジタル・フォレンジックにおける問題、そして、暗号化型ランサムウェアや組織内部での不正なSC削除からファイルを保護するために、SCを利用したファイル管理システムを提案した。本稿が提案するVSSManagerは、エンドユーザ用のバックアップ機能と組織用のSC管理機能から構成されるシステムである。今回は、エンドユーザ用バックアップ機能の有用性を確かめるためにプロトタイプを開発して実験と評価を行った。バックアップの基本的な機能は、一般ユーザが容易に利用できるようにユーザインタフェースを検討して実装した。テストユーザによるアンケートでは、従来までのSC関連ツールに比べて使いやすいという評価が得られた。また、SC保護機能の評価実験では、SC削除攻撃を行うランサムウェアに対して有効な機能であることを証明した。これらの結果から、エンドユーザ用ツールとして有効性があると考えられる。最後に、VSSはWindows OSのサービスであるが、スナップショット機能が実装されているUnix系システムであれば、本稿が提案する仕組みを応用することができると考える。

参考文献

- [1] 佐々木良一, 上原哲太郎, 櫻庭信之, 白濱直哉: デジタル・フォレンジックの基礎と実践, p.266, 東京電機大学出版局 (2017).
- [2] 山前 碧, 小林裕太, 上原哲太郎, 佐々木良一: SSD上の消去ファイルの復元可能性の実験と評価, 情報処理学会研究報告, Vol.2015-DPS-162, No.39, pp.1–7 (2015).
- [3] 吉田哲平, 小高知宏, 黒岩丈介, 白井治彦: P2Pを利用したデータバックアップシステムの提案, 福井大学大学院工学研究科研究報告, Vol.64, pp.57–63 (2016).
- [4] Rahumed, A. et al.: A Secure Cloud Backup System with Assured Deletion and Version Control, *International Conference on Parallel Processing Workshops*, pp.160–167 (2011).
- [5] Volume Shadow Copy Service, available from <https://msdn.microsoft.com/ja-jp/library/windows/desktop/bb968832%28v=vs.85%29.aspx> (accessed 2017-10-21).
- [6] Pecherle, G. et al.: Methods of Isolation for Application Traces Using Virtual Machines and Shadow Copies, *International Journal of Advanced Computer Science and Applications*, Vol.5, pp.33–37 (2014).
- [7] Windows Shadow Volumes, available from http://www.forensicswiki.org/wiki/Windows_Shadow_Volumes (accessed 2017-11-23).
- [8] ランサムウェアによる攻撃を受けたユーザー, 前年比17.7%増の230万超へ, 入手先 (<http://www.kaspersky.co.jp/about/news/virus/2016/vir28062016>) (参照 2017-10-21).
- [9] 竹林康太, 上原哲太郎, 佐々木良一: ライブフォレンジックを用いた暗号化ファイル復元技術の開発, 情報処理学会研究報告, Vol.2015-DPS-162, No.38, pp.1–6 (2015).
- [10] Mbol, F. et al.: An Efficient Approach to Detect Torrent-Locker Ransomware in Computer Systems, *International Conference on Cryptology and Network Security* pp.532–541 (2016).
- [11] 削除したファイルを以前のバージョンから復元する方法, 入手先 (<https://www.microsoft.com/ja-jp/atlife/tips/archive/windows/tips/311.aspx>) (参照 2016-10-31).
- [12] ShadowExplorer.com, available from (<http://www.shadowexplorer.com/>) (accessed 2016-10-31).
- [13] 拡大する WannaCry ランサムウェアの分析, 入手先 (<http://blogs.mcafee.jp/wannacry-f851>) (参照 2017-10-21).
- [14] Zepto ransomware now introduces new features to better encrypt your files, available from (<https://blog.avast.com/zepto-ransomware-now-introduces-new-features-to-better-encrypt-your-files>) (accessed 2017-10-21).



松高 直輝

東京電機大学。2016年東京電機大学未来科学部情報メディア学科卒業。同年同大学大学院未来科学研究科情報メディア学専攻に進学。サイバーセキュリティの研究に従事。



松本 隆

東京電機大学。セキュリティ事業者にてフォレンジックエンジニア, 大手SIerでのセキュリティエンジニアを経て, 2018年よりDeNAでグループのSOCやOSINTチーム立ち上げを担当。特定非営利活動法人デジタル・フォレンジック研究会理事, 東京電機大学サイバー・セキュリティ研究所客員研究員等。



上原 哲太郎 (正会員)

立命館大学. 1995 年京都大学大学院工学研究科博士後期課程研究指導認定退学. 同年同大学院工学研究科助手. 1996 年和歌山大学情報処理センター講師. 2000 年同大学システム工学部講師. 2003 年京都大学工学研究科附属情報センター助教授. 2006 年同大学学術情報センター助教授. 2011 年総務省通信規格課標準化推進官. 2013 年より現職. システムセキュリティ, デジタル・フォレンジック等の研究開発に従事. 京都大学博士 (工学). 共著に『IT Text ネットワークセキュリティ』等.



佐々木 良一 (正会員)

東京電機大学. 1971 年東京大学卒業. 同年日立製作所入社. システム開発研究所でセキュリティ技術, ネットワーク管理システム等の研究開発に従事. 2001 年より 2018 年まで東京電機大学教授, 現在, 同大学特命教授, 工学博士 (東京大学). 2002 年情報処理学会論文賞受賞. 2007 年および 2017 年に総務大臣表彰等. 著書に, 『IT リスクの考え方』(岩波新書, 2008 年) 等. 日本セキュリティ・マネジメント学会会長, 内閣官房サイバーセキュリティ補佐官等を歴任. 本会フェロー.